Amendments to the Drawings

Replacement drawings for Figs. 2 and 3 are being submitted herewith to replace the originally filed drawings.

Attachment: Replacement Sheets
Annotated Marked-Up Drawings

REMARKS

Claims 1-22 are pending in the application. Claims 1 and 17 are independent claims. Claims have been rejected under 35 U.S.C. 102(e). Those rejections are respectfully traversed and reconsideration is requested.

Drawings

The examiner noted on page 2 of the Office Action that reference number 360 on page 7 of the Applicants' Specification is not indicted in corresponding Fig. 2. Accordingly, Fig. 2 has been amended to include reference number 360. Fig. 3 has also been amended to correct a typographical error.

Rejections under 35 U.S.C. 102(e)

Claims 1-22 have been rejected under 35 U.S.C. 102(e) as being anticipated by Belfiore (U.S. Patent No. 6,990,513).

Before discussing the cited references, however, a brief review of the Applicants' disclosure may be helpful without limiting the claims. The Applicants' disclosure is directed to a method and system for journaling activity in a data processing system. Referring to Figs. 2 and 3, An agent process 300 runs in the background of a client operating system kernel 102 and interrupts requests for access to resources. The agent process 300 contains sensors 500 that capture low level system events 350, 510, such as file read, file write, clipboard copy, CD-RW access, TCP/IP network message outbound, and the like. The low level events 350, 510 are then associated with one or more file names, and a filter 520 filters the events 350, 510 against an approved list, removing references to approved files, such as operating system files, that do not contain sensitive application data. A coalescer 530 further processes atomic events 350, 510 associated with, or related to, a single user action. For example, a typical pattern of file access is a "file open" atomic event followed by multiple "file read" atomic events to the same file. If such a sequence of atomic events 350, 510 occurs from the same process and the same executable with the same thread ID and the same file name, the coalescer 530 counts only a single "FileOpen" event. The resulting events are then bundled together and sent securely to a

journaling server 104-2 that examines the events to determine an aggregate event 360 that may indicate a possible abuse of trust situation. For example, an aggregate "FileEdit" event might be reported by the journaling server 104-2 when a user has opened and modified a sensitive financial document, with that user then printing the document, renaming it, and saving it to a newly attached USB hard drive.

Turning to the cited reference, Belfiore discusses a method for fulfilling requests in a server federation. The method includes an events component that facilitates the communication of events between software components (i.e., event sources and event sinks) that generate and receive event notifications.

Belfiore does not teach or suggest *"a sensor to sense atomic level events, the sensor located within an operating system kernel within a user client device"* as now claimed in independent Claim 1. While Belfiore discloses event sources that generate atomic events that are then provided to an event composition mechanism, Belfiore does not disclose that the event sources capture or sense the atomic events. Moreover, Belfiore does not disclose that the event sources are located within an operating system kernel within a user client device. (See Belfiore col. 20, lines 46-60.)

Furthermore, Belfiore does not teach or suggest *"an aggregator to accept multiple atomic level events and to generate an aggregate event based on a predetermined sequence of atomic level events"* as now claimed in independent Claim 1. While Belfiore discloses an event composition mechanism that transforms atomic events into higher-level events, Belfiore does not disclose that the event composition mechanism generates the higher-level events based on a predetermined sequence of atomic level events. (See Belfiore col. 20, line 57 – col. 21, line 12.)

Independent Claim 17 is similar to Claim 1 and should be found in allowable condition for the same reasons as discussed above for independent Claim 1.

Dependent Claims 2-16 and 18-22 are directly or indirectly dependent on independent Claims 1 or 17 and thus are novel over the cited art for at least the same reasons as discussed above for independent Claims 1 and 17.

Furthermore, dependent Claims 2-16 and 18-22 recite further limitations that are neither taught nor suggested by the cited art. For example, Belfiore does not teach or suggest *"filtering atomic level events with an approved event list"* as claimed in Claims 4 and 18. While Belfiore

discloses filtering atomic events into higher-level events (see Belfiore col. 21, lines 4-7), Belfiore does not disclose the use of an approved events list for filtering the events. The informational requirements of the software components of Belfiore do not meet the limitation of the approved events list, as the informational requirements merely define the level of abstraction at which the software components may make decisions. The requirements are not an approved events list.

Further, Belfiore does not teach or suggest that the *"approved event list includes a list of approved file identifiers"* as claimed in Claims 5 and 19, as Belfiore does not teach or suggest the subject matter of Claims 4 and 18, from which Claims 5 and 19 depend. Moreover, even if Belfiore did disclose an approved event list that was stored in an event store, the list would merely be associated with a file identifier, and would not teach or suggest that the approved events list include a list of approved file identifiers.

Further, Belfiore does not teach or suggest that the *"file identifiers are a hash code"* as claimed in Claim 6, as Belfiore does not teach or suggest the subject matter of Claims 4 or 5 from which Claim 6 depends. Moreover, Belfiore does not teach or suggest the use of a hash code.

Further, Belfiore does not teach or suggest *"a coalescer to coalesce multiple atomic events output by the sensor into a single event prior to inputting them to the aggregator"* as claimed in Claim 8 and as similarly claimed in Claim 21. While Belfiore discloses an event composition mechanism that transforms atomic events into higher-level events, Belfiore does not disclose a coalescer that coalesces atomic events into a single event prior to inputting them to the composition mechanism. Moreover, the mere presence of multiple parallel arrows between Belfiore's event sources and the composition mechanism (see Belfiore, Fig. 5, ref. no. 606) do not teach or suggest a coalescer as claimed in Claims 8 and 21.

Further, Belfiore does not teach or suggest that *"a bundle of coalesced events is created prior to their transmission between the agent and the server"* as claimed in Claim 9 and as similarly claimed in Claim 22, as Belfiore does not teach or suggest the subject matter of Claims 8 or 21 from which Claims 9 and 22 depend. Moreover, even if the event composition mechanism of Belfiore were to be construed as creating a bundle of coalesced events, the bundle would not be created before transmission to the composition mechanism.

Further, Belfiore does not teach or suggest that *"aggregate events are used to control security of the data processing system"* as claimed in Claim 14. While it is disclosed that the event component of Belfiore uses the security component of Belfiore (see Belfiore, col. 21, lines 50-53), it is not disclosed that the events of Belfiore's event component are used to control security.

Further, Belfiore does not teach or suggest that *"aggregate events are used to provide a perimeter of accountability for file usage at a point of system use"* as claimed in Claim 15. A perimeter of accountability is different from security, thus, while Belfiore discusses security, Belfiore does not disclose a perimeter of accountability.

As such, the 35 U.S.C. 102(e) rejections of Claims 1-22 are believed to be overcome. Accordingly, the present invention as claimed is not believed to be anticipated or made obvious from the cited or prior art. Removal of the rejections under 35 U.S.C. 102(e) and acceptance of Claims 1-22 is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By_____

David J. Thibodeau, Jr.
Registration No. 31,671
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Date: 5/14/07